

January 19, 2007

Office of the Secretary  
Federal Trade Commission  
Room H-135 (Annex N)  
600 Pennsylvania Avenue, N.W.  
Washington, DC 20580

Re: Identity Theft Task Force P065410

To Whom It May Concern:

This letter is submitted by the Consumer Bankers Association ("CBA") in response to the request for comment ("Request") issued by the Identity Theft Task Force ("Task Force"). The CBA is the recognized voice on retail banking issues in the nation's capital. Member institutions are the leaders in consumer financial services, including auto finance, home equity lending, card products, education loans, small business services, community development, investment and deposits. CBA was founded in 1919 and provides leadership, education, research and federal representation on retail banking issues such as privacy, fair lending, and consumer protection legislation/regulation. CBA members include most of the nation's largest bank holding companies as well as regional and super community banks that collectively hold two-thirds of the industry total assets.

The Request touched on general issues of identity theft prevention, mitigation, and enforcement. We will address issues in the order they were presented in the Request, and we thank the Task Force for allowing us to provide our comments.

## **Maintaining Security of Consumer Data**

### *Use of SSNs*

Public and private sector entities rely on SSNs to assist in the authentication of individual identities as well as ensure the proper matching of information to an individual's records. The SSN is an important tool with respect to both of these objectives insofar as it is the only unique identifier assigned to every individual. Unlike any other piece of information created by the government or private sector, the SSN is constant and widely relied upon. The SSN therefore serves as a critical piece of information when trying to verify an individual's identity or match records for that individual.

The SSN is used in millions of circumstances to prevent fraud or enhance the accuracy of consumer information. If the SSN did not exist, the private sector would have to create a similar unique identification system, which would pose the exact same issues as are posed by use of the SSN.<sup>1</sup> The public and private sectors need additional information other than name, address, or other readily obtainable (and therefore unreliable for fraud protection) information in order to provide constituents and consumers efficient and accurate service.

We note that reliance on SSNs is generally effective only because SSNs are viewed to be reasonably reliable with respect to their integrity. In other words, they are not as widely available as other forms of identification, such as an individual's name or address and therefore more difficult for criminal to misuse. The public and private sectors therefore have obvious interests in protecting the integrity of SSNs so as to be able to continue to rely on them for constituent and consumer transactions. CBA applauds the Task Force for investigating the current use and collection of SSNs with an eye toward preserving their integrity.

---

<sup>1</sup> We also note that biometrics could be used to serve as a universal identifier, but the use of biometrics raises a host of other legitimate issues for consideration.

The Task Force appears to believe that a reduction in the collection and use of SSNs will preserve the integrity and reliability of SSNs. This may be true, but only to a limited extent. For example, limitation of the public display of SSNs (such as identification badges) may provide some protection for SSNs. On the whole, however, CBA does not necessarily believe that a limitation on the collection or use of SSNs would be nearly as effective as protecting the SSN once it is collected. Furthermore, we have significant concerns about attempting to ascertain the difference between legitimate/appropriate needs for SSNs and frivolous/unnecessary uses. This is not as simple as it may sound, and the risks associated with imposing too many limitations on SSNs far outweigh any benefits there may be in restricting the SSN's use.

### *Data Security*

The Task Force is already aware that the Gramm-Leach-Bliley Act ("GLBA") requires financial institutions to adopt information safeguarding programs designed to protect "nonpublic personal information" against a variety of threats. In fact, the federal banking agencies and the Federal Trade Commission ("FTC") have implemented this requirement in an effective manner that deserves review by the Task Force. CBA believes that the importance of data security depends not on the type of entity that possesses the consumer information, but the type of consumer information possessed. We believe that sensitive information, such as a consumer's name and account number, should be subject to data security requirements, regardless of whether the entity possessing the information is a financial institution, government agency, or any other entity. CBA therefore supports applying information safeguarding requirements, similar to those applicable to financial institutions, to all entities. For ease of compliance and consistent application, such requirements should be a national uniform standard enforced administratively by federal agencies. To the extent the new standard deviates from the GLBA requirements, we believe financial institutions should be deemed to be in compliance with the federal standard to the extent they are in compliance with the GLBA standard. The existing GLBA standards have proven satisfactory, the federal banking regulators have developed sophisticated examination procedures and financial institutions should not be required to undertake another information safeguarding project.

### *Data Breach Notification*

As with data security, banks already have data breach notification requirements under the GLBA. As a general matter, CBA believes these requirements are reasonable and should be given consideration for any broadly applicable requirement reviewed by the Task Force. If the Task Force intends to recommend a federal data breach notification standard, we believe it should establish national uniform requirements and be enforced administratively by federal agencies. We also believe it should have an appropriate "trigger" before notices are required. For example, a notice should not be required simply because there was a data breach or consumers will become "numb" to the notifications. Rather, consumers should receive notice only when they are at a significant risk for harm as a result of the data breach. Finally, as with data security, we believe that banks should have the option of complying with the existing data breach notification interpretations of the federal banking agencies.

## **Preventing the Misuse of Consumer Data**

The Task Force has recommended holding a workshop or a series of workshops involving a wide variety of interested parties focused on developing and promoting improved means of authenticating the identities of individuals. We encourage the Task Force to hold as many of these symposia as possible. It is important to learn about the existing efforts, both voluntary and legally required, to authenticate individual identities. It seems that, at times, there is a general misunderstanding with respect to the efforts that companies, especially banks, make to authenticate individual identities. Indeed, it is usually the bank that suffers the financial harm associated with financial fraud. Banks therefore have every incentive to ensure that they know the true identity of the individual with whom they are dealing. Yet existing identity verification techniques are obviously not foolproof. CBA believes that both the public and private sector could learn significant amounts of information with respect to the evolution of identification authentication methods through these workshops.

## Victim Recovery

As a general matter, CBA does not have specific comments with respect to several of the items raised in connection with victim recovery. We do believe it would be important for the Task Force to assess existing protections with respect to identity theft mitigation measures, including those in the Fair Credit Reporting Act ("FCRA"), as amended by the FACT Act. Despite significant bi-partisan support, including from the Bush Administration, the identity theft mitigation measures included in the FACT Act have not been widely discussed nor have they been evaluated by Congress or the Administration. In fact, identity theft victims have *extraordinary* powers under the FCRA to clean up their credit history and force creditors to engage in due diligence before granting credit in identity theft victims' names. Many of these tools were policy objectives of the Bush Administration, and they deserve attention. CBA believes that if policymakers should have the opportunity to carefully consider the panoply of rights and powers granted to identity theft victims, before adopting some of the more extreme policy proposals (e.g., credit freeze laws) that could inadvertently create more problems than they solve.

CBA supports the Task Force's initiative to seek additional information regarding credit freeze laws before coming to any conclusion on the matter. We believe that credit freeze laws are harmful to many consumers insofar as they thwart legitimate credit applications to the same extent they thwart fraudulent applications. We strongly urge the Task Force to include in its consideration the impact credit freeze proposals have on consumers who need instant credit, or other forms of credit, but are unable to "thaw" the freeze. We note that there are many issues that arise in this regard, such as in connection with mortgage financing. CBA believes that given the current protections afforded consumers under the FCRA, it is unnecessary to enact credit freeze requirements. To the extent the Task Force disagrees, we hope the Task Force's recommendation recognizes the difficulties inherent in freezing a credit file. For example, perhaps victims of identity theft should be the only people able to freeze their file. Regardless, it would be important for any federal credit freeze law to establish a national uniform standard.

## Law Enforcement

### *National Identity Theft Law Enforcement Center*

Though it may be appropriate to create a nationwide clearinghouse dedicated to assisting law enforcement and the private sector in connection with preventing, investigating, and prosecuting identity theft crimes, the logistics of such a program may be difficult to sort through, especially as they relate to issues of civil liberties (from the consumer's perspective) and protecting sensitive information (from law enforcement's perspective).

### *Ability of Law Enforcement to Receive Information from Financial Institutions*

We believe that financial institutions are obviously an important source of information in connection with identity theft investigations. To our knowledge, there are few if any legal impediments with respect to law enforcement's ability to obtain information it needs to investigate and prosecute identity theft. To the extent that law enforcement has difficulty under the existing legal requirements (e.g., the Right to Financial Privacy Act, the FCRA), CBA stands ready to discuss these issues with the relevant law enforcement agencies. Banks have every incentive to investigate and prosecute identity thieves, and are generally willing to provide information sought by law enforcement. CBA asks that, if the Task Force recommends changes to the existing ability of law enforcement to obtain information from financial institutions, that financial institutions be shielded from liability in connection with providing such information to law enforcement.

### *Prosecutions of Identity Theft*

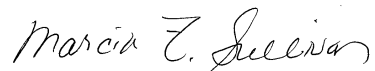
CBA strongly supports efforts to increase the number of identity theft investigations and prosecutions. We would leave the specific recommendations as to how this objective may be achieved to those with expertise in this area. However, it is fair to say that law enforcement appears to have insufficient

manpower and monetary resources to tackle the identity theft issue and the lack of prosecution is severely limiting efforts to reduce identity theft.

\* \* \* \* \*

Once again, CBA appreciates the opportunity to provide comments in response to the Request. Please do not hesitate to contact Marcia Sullivan at 703-276-3873 if we may be of further assistance in this matter.

Very Truly Yours,

A handwritten signature in cursive script that reads "Marcia Z. Sullivan".

Marcia Z. Sullivan  
Director, Government Relations